# Research Proposal - Cybersecurity and Crime

Mundher Al-Ahmadi

May 8, 2023

## 1 Introduction

The number of internet users has been steadily on the rise and projected to continue to rise. As digitalization expands, particularly since the outbreak of COVID-19, instances of cybercrime have similarly been increasing [7], despite being significantly underreported. [3] This raises many questions about cybercrime and security. Among those questions is the effect of cybercrimes such as phising and identity theft on victims.

## 2 Background and Significance

### 2.1 Costs of Cybercrime

The amount of internet users world-wide has increased from about 1 billion to 5.3 billion in the period between 2005 and 2022. [8] This figure is expected to continue growing, as well as cybercrime [6], although it is severely underreported. Cybercrime has very significant financial costs that are also projected to increase at a high rate. According to the Europol's Internet Organized Crime Threat Assessment (IOCTA) [3], cybercrime is becoming more aggressive and confrontational. Such crimes include but are not limited to cyberstalking, sexual extortion as well as child abuse. The effects of such crimes can be very severe. [3]

Many cybercrimes are carried out at a mass scale with very low costs. For example, phising attacks can be carried out with very little cost. Another example are DDoS attacks. DDoS attacks are performed by bots, are accessible to any individual, and can be carried out for as little as 10 USD. [4] There

are many estimations on the financial costs of such attacks on individuals and companies, and they seem to be significant. Cybercrimes are estimated to cost the world economy about 8 trillion USD in 2023. [9]

The psychological effects of such crimes are also relevant. Victims report feelings of that range from shame and embarrassment to shock and even trauma. Jansen and Leukfeldt report some coping mechanisms that phishing victims use. The first coping mechanism was reporting the crime to their bank. Victims also change their online environment by more frequently installing software security updates. While these coping strategies are problem-focused, they could instill a feeling of security and confidence when using online banking. Another coping mechanism is emotion-focused, which is to tell friends and family about the incident. Though, a victim reports that their feelings about the incident prevented them from telling anyone. [5]

## 2.2 Problem scaling

The growth of internet usage and the rate of cybercrime is a cause for great concern for a number of reasons:

1. a 6% compound annual growth rate in internet users introduces billions of new potential victims. [8]
2. Limited levels of awareness against cybercrime prevention. [2]
3. Unknown levels of awareness about the psychological and financial damages to victims.

The sum of these reasons implies a highly neglected cause. However, there is reason to believe that there is much potential for things to improve. The number of unfilled cybersecurity jobs has grown from one million to 3.5 million between 2013-2021. [9] McKinsey believes that there may be a big addressable market for cybersecurity. As of 2021, The total addressable market is predicted to be valued between 1.5 trillion to 2 trillion dollars, which is about 10 times as big as the vended market. [1] There has also been developments in rethinking cybersecurity models and frameworks with companies like RSA focusing on identity authentication and authorization. Although this might mean a great deal of potential for innovations in prevention, it has no implications for financial and psychological recovery for victims.

# 3 Research Methods

A keyword search analysis will be performed as a means to measure the amount of research on the topic of cybercrime victmization. Furthermore, literature on the topic will be examined and a topical analysis using Latent Dirichlet Allocation (LDA) will be performed on text data from existing literature, as well as on posts from online forums and social media platforms. Using LDA, the topics of discussion will be identified.

# 4 Expected Outcomes

The analysis will provide a topic model of the discussion on cybercrime victimization. The model can be used to identify the most discussed topics, as well as the most neglected topics. This facilitates literature reviews and supports hypothesis generation.

# References


[1] Bharath Aiyer, Jeffrey Caso, Peter Russell, and Marc Sorel. New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers. *McKinsey & Company*, October 27 2022.

[2] EGA ENISA. Raising awareness of cybersecurity. Event Proceedings, November 2021.

[3] Europol. Internet organised crime threat assessment (iocta) 2021, 2021.

[4] Miguel Gomez. Dark web price index 2020. Technical report, 2020.

[5] Jurjen Jansen and Rutger Leukfeldt. Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology*, 6(2):205–228, 2018.

[6] Grainne H. Kirwan. The Rise of Cybercrime. In *The Oxford Handbook of Cyberpsychology*. Oxford University Press, 05 2019.

[7] Samantha Monteith, Michael Bauer, Martin Alda, and et al. Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports*, 23(3):18, 2021.

[8] Statista. Number of internet users worldwide from 2005 to 2021 (in millions), 2022.

[9] Cybersecurity Ventures. 2022 official cybercrime report, 2022.